ABSTRACT

A method and apparatus are disclosed for generating random numbers using the meta-stable behavior of flip-flops. A flip-flop is clocked with an input that deliberately violates the setup or hold times (or both) of the flip-flop to ensure meta-stable behavior. When a meta-stable event is detected, an output bit is provided as a random bit. An even random number distribution is obtained by "marking" half of the zeroes input to the flip-flop as "ones" and the other half of the zeroes as "zeroes." In addition, half of the ones are marked as "ones" and the other half of the ones are marked as "zeroes." The marking signal is uncorrelated to any noise to a high probability using a linear feedback shift register.